UNITED STATES DISTRICT COURT

FOR THE WESTERN DISTRICT OF NEW YORK

PETER TASSMER and KAREN CANNON individually, and on behalf of a class of others similarly situated, Plaintiffs, v. PROFESSIONAL BUSINESS SYSTEM d/b/a PRACTICEFIRST MEDICAL MANAGEMENT SOLUTIONS and PBS MEDCODE CORP. a Delaware corporation, Defendant.	:	Civil Action No. _____ **CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

Plaintiffs Peter Tassmer and Karen Cannon individually, and on behalf of all others similarly situated, upon personal knowledge of the facts pertaining to them and on information and belief as to all other matters, by and through the undersigned counsel, hereby bring this Class Action Complaint against Defendant Professional Business Systems d/b/a Practicefirst Medical Management Solutions and PBS Medcode Corp. ("Practicefirst" or "Defendant"), and allege as follows:

INTRODUCTION

1. Practicefirst is a medical management solutions company that touts itself as a "leader in billing, credentialing, coding, compliance, chart auditing, bookkeeping and tax preparation."[1]

2. Practicefirst provides administrative and back-office services to medical professionals and takes "responsibility to stay current with the volatile rules, regulations and information technology requirement of the healthcare industry."[2]

3. However, because of Practicefirst's unsecure and inadequate data security practices, an unauthorized third party accessed and compromised files from Practicefirst's system that included patient and employee data (the "Data Breach") of over 1.2 million individuals. It is unclear for how long this data theft took place, but Defendant "discovered" it on December 30, 2020.

4. Although information accessed and stolen varied by individual, the categories of patient and employee data obtained by the hackers included: names, addresses, email addresses, dates of birth, driver's license numbers, Social Security numbers, diagnoses, laboratory and treatment information, patient identification numbers, employee username and passwords, employee username with security

[1] https://www.practicefirstsecure.com/about
[2] *Id*.

questions and answers, and bank account and/or credit card/debit card information.[3] This information is known as Protected Healthcare Information ("PHI") or Personally Identifiable Information ("PII") and is of significant value to cyber criminals.

5. On July 1, 2021, over six months after discovering the Data Breach, Practicefirst notified the Attorney General of several states, including Maine and California, of the breach. Around the same time, Practicefirst also began sending notices to patients and employees whose PII/PHI may have been impacted by the Data Breach.

6. Due to Practicefirst's carelessness and inadequate security, Plaintiffs and the Class have suffered irreparable harm and are subject to an increased risk of identity theft. Plaintiffs and the Class' PII/PHI has been compromised and they must now undertake additional ongoing security measures to minimize the risk of identity theft.

PARTIES

7. Plaintiff Peter Tassmer resides in New Britain, in the State of Connecticut, County of Hartford.

8. Plaintiff Karen Cannon resides in Dunkirk, in the State of New York.

9. Defendant Professional Business Systems d/b/a Practicefirst Medical Management Solutions and PBS Medcode Corp. "Practicefirst" is a Delaware

[3] https://www.practicefirstsecure.com/security-incident

Corporation headquartered in New York. Its principal place of business is at 275 Northpointe Parkway, Suite 50, Amherst, NY, 14228.

JURISDICTION AND VENUE

10. The Court has subject matter jurisdiction over this case pursuant to the Class Action Fairness Act, 28 U.S.C. § 1332(d), because at least one member of the proposed class is a citizen of a state different from one of the Defendant's home state, the number of proposed class members exceeds 100, and the aggregate amount in controversy exceeds $5,000,000, exclusive of interest and costs.

11. The Court has personal jurisdiction over Defendant because it conducts business in New York, and it is headquartered in Amherst, New York.

12. Venue is also proper in this District pursuant to 28 U.S.C. § 1391(b) because Defendant resides in this district and regularly conduct business in this district, a substantial part of the events and/or omissions giving rise to Plaintiffs' and the Class members' claims occurred within this district, and Defendant has caused harm to class members residing in this district.

FACTUAL ALLEGATIONS

13. As a medical management solutions business focused on the efficiency, accuracy, and security of the data it processes for health care providers, Practicefirst has both the duty and the means to provide secure systems for the sensitive healthcare billing and coding services it provides. Plaintiffs and the Class had a reasonable

expectation that Practicefirst would secure the information it processed and maintained.

14. However, on or about July 6, 2021, Plaintiffs and Class members were notified their PII/PHI had been "copied by an unauthorized actor before it was permanently deleted," according to the notice submitted to the Office of the Attorney General for the State of California.

15. Practicefirst has waited over six months before notifying Plaintiffs and Class Members that they may have been victims of the data breach. This delay in notification to Plaintiffs and Class members gave the hackers time to use the stolen PII/PHI without restriction, further harming Plaintiffs and Class members.

16. Practicefirst failed to protect Plaintiffs and Class members by failing to employ the appropriate security to detect intrusions, allowing the hackers to steal the most private and sensitive information from patients and employees. Plaintiffs and Class members can reasonably believe that the risk of future harm (including identity theft) is substantial and imminent, and will need to take steps to mitigate that substantial risk of future harm.

A. Plaintiffs' experiences

17. Plaintiff Tassmer received notice of the Data Breach on or about July 3, 2021. Plaintiff Tassmer had never heard of Practicefirst prior to receiving the notice.

18. The letter from Practicefirst instructed Plaintiff Tassmer to, among other things, "regularly review account statements and report any suspicious activity to financial institutions." It also provided him an option to enroll in credit monitoring and identity theft recovery services.

19. After receipt of the Notice letter, Plaintiff Tassmer made reasonable efforts to mitigate further impact of the Data Breach. He spent time researching the Data Breach, reviewing and monitoring his credit reports and financial account statements for any indications of actual or attempted identity theft or fraud. This is valuable time he otherwise would have spent on other activities.

20. Plaintiff Tassmer suffered additional actual injury from having his PII/PHI compromised in the Data Breach including, but not limited to (a) damage to and diminution in the value of his PII, a form of property that Defendant had possession of; (b) violation of his privacy rights; and (c) further imminent and impending injury arising from the increased risk of identity theft and fraud.

21. Plaintiff Cannon received notice of the Data Breach on or about July 3, 2021. Plaintiff Cannon had never heard of Practicefirst prior to receiving the notice.

22. The letter from Practicefirst instructed Plaintiff Cannon to, among other things, "regularly review account statements and report any suspicious activity to financial institutions." It also provided her an option to enroll in credit monitoring and identity theft recovery services.

23. After receipt of the Notice letter, Plaintiff Cannon made reasonable efforts to mitigate further impact of the Data Breach. She spent time researching the Data Breach, reviewing and monitoring her credit reports and financial account statements for any indications of actual or attempted identity theft or fraud. This is valuable time she otherwise would have spent on other activities.

24. Plaintiff Cannon suffered additional actual injury from having her PII/PHI compromised in the Data Breach including, but not limited to (a) damage to and diminution in the value of her PII/PHI, a form of property that Defendant had possession of; (b) violation of her privacy rights; and (c) further imminent and impending injury arising from the increased risk of identity theft and fraud.

B. The PHI/PII stolen in the Data Breach is incredibly valuable to data thieves and allows for identity fraud

25. The personal, health, and financial information of consumers, such as Plaintiffs and Class members, is valuable and has been commoditized in recent years.

26. The repercussions of Practicefirst's failure to keep Plaintiffs' and Class members' PII/PHI secure are severe. Identity theft occurs when someone uses another's personal and financial information such as that person's name, account number, Social Security Number, date of birth, and/or other information, such as health insurance or prescriptions, without permission, to commit fraud amongst other crimes.

27. According to experts, one out of four data breach notification recipients become a victim of identity fraud.

28. Stolen PHI/PHI is often trafficked on the "dark web," a heavily encrypted part of the Internet that is not accessible via traditional search engines. This is because malicious actors buy and sell that information for profit.[4] Law enforcement has difficulty policing the "dark web" due to this encryption, which allows users and criminals to conceal identities and online activity.

29. Once PII/PHI is sold, it is often used to gain access to various areas of the victim's digital life, including bank accounts, social media, credit card, and tax details. This can lead to additional personally identifying information being harvested from the victim, as well as information from family, friends and colleagues of the original victim.

30. According to the FBI's Internet Crime Complaint Center (IC3) 2019 Internet Crime Report, Internet-enabled crimes reached their highest number of complaints and dollar losses that year, resulting in more than $3.5 billion in losses to individuals and business victims.

31. Further, according to the same report, "rapid reporting can help law enforcement stop fraudulent transactions before a victim loses the money for good."

[4] *Shining a Light on the Dark Web with Identity Monitoring*, IdentityForce, Dec. 28, 2020, *available at*: https://www.identityforce.com/blog/shining-light-dark-web-identity-monitoring (last visited July 7, 2021).

Waiting over six months to notify Plaintiffs and Class members that their PII/PHI had been stolen is far from rapid reporting.

32. Victims of identity theft also often suffer embarrassment, blackmail, or harassment in person or online, and/or experience financial losses resulting from fraudulently opened accounts or misuse of existing accounts.

33. Data breaches facilitate identity theft as hackers obtain patients' PII/PHI and thereafter use it to perpetrate health insurance fraud, siphon money from current accounts, open new accounts in the names of their victims, or sell consumers' PII/PHI to others who do the same.

34. For example, the United States Government Accountability Office noted in a June 2007 report on data breaches (the "GAO Report") that criminals use PII to open financial accounts, receive government benefits, and make purchases and secure credit in a victim's name.[5] The GAO Report further notes that this type of identity fraud is the most harmful because it may take some time for a victim to become aware of the fraud, and can adversely impact the victim's credit rating in the meantime. The GAO Report also states that identity theft victims will face "substantial costs and inconveniences repairing damage to their credit records . . . [and their] good name."[6]

---

[5] *See* Government Accountability Office, Personal Information: Data Breaches are Frequent, but Evidence of Resulting Identity Theft is Limited; However, the Full Extent is Unknown (June 2007), available at http://www.gao.gov/assets/270/262899.pdf (last visited July 7, 2021).

[6] *Id.*

35. Moreover, in light of the current COVID-19 pandemic, Plaintiffs' sensitive information could be used to fraudulently obtain any emergency stimulus or relief payments or any additional forms monetary compensation, unemployment and/or enhanced unemployment benefits.

36. Victims of identity theft often suffer indirect financial costs as well, including the costs incurred due to litigation initiated by creditors and in overcoming the many obstacles they face in obtaining or retaining credit.

37. In addition to out-of-pocket expenses that can exceed thousands of dollars for the victim of new account identity theft, and the emotional toll identity theft can take, some victims have to spend a considerable time repairing the damage caused by the theft of their PII/PHI. Victims of new account identity theft will likely have to spend time correcting fraudulent information in their credit reports and continuously monitor their reports for future inaccuracies, close existing bank/credit accounts, open new ones, and dispute charges with creditors.

38. Medical data, like Plaintiffs' and Class members' PII/PHI, is also especially valuable to identity thieves. According to a 2012 Nationwide Insurance report, "[a] stolen medical identity has a $50 street value..."[7] In fact, the medical

[7] Study: Few Aware of Medical Identity Theft Risk, Claims Journal, https://www.claimsjournal.com/news/national/2012/06/14/208510.htm (last visited July 7, 2021).

industry has experienced disproportionately higher instances of data theft than any other industry.

39. Medical identity theft is one of the forms of identity theft that is most common, most expensive, and most difficult to prevent. According to Kaiser Health News, "medical-related identity theft accounted for 43 percent of all identity thefts reported in the United States in 2013," which is more "than identity thefts involving banking and finance, the government and the military, or education."[8]

40. As indicated by Jim Trainor, second in command at the FBI's cyber security division: "Medical records are a gold mine for criminals – they can access a patient's name, DOB, Social Security and insurance numbers, and even financial information all in one place."[9]

41. Further complicating the issues faced by victims of identity theft, data thieves may wait years before attempting to use the stolen PII/PHI. To protect themselves, Plaintiffs and Class members (and the business entities whose information was breached) will need to be remain vigilant against unauthorized data use for years or even decades to come.

---

[8] Michael Ollove, "The Rise of Medical Identity Theft in Healthcare," Kaiser Health News, Feb. 7, 2014, https://khn.org/news/rise-of-indentity-theft/ (last visited July 7, 2021).

[9] IDExperts, You Got It, They Want It: Criminals Targeting Your Private Healthcare Data, New Ponemon Study Shows, https://www.idx.us/knowledge-center/you-got-it-they-want-it-criminals-are-targeting-your-private-healthcare-dat (last visited July 8, 2021).

42. The FTC has also recognized that consumer data is a new (and valuable) form of currency. In a recent FTC roundtable presentation, another former Commissioner, Pamela Jones Harbour, underscored this point: Most consumers cannot begin to comprehend the types and amount of information collected by businesses, or why their information may be commercially valuable. Data is currency.

43. Recognizing the high value consumers place on their PII/PHI, many companies now offer consumers an opportunity to sell this information to advertisers and other third parties. The idea is to give consumers more power and control over the type of information they share and who ultimately receives the information. And, by making the transaction transparent, consumers—not criminals—will be compensated.[10]

44. Consumers, such as Plaintiffs and members of the Class, place a high value on their PII and a greater value on their PHI. Research shows how much consumers value their data privacy, and the amount is considerable. Indeed, studies confirm that "[a]mong U.S. subjects, protection against errors, improper access, and secondary use of personal information is worth US $30.49–44.62."[11]

---

[10] *See* Steve Lohr, You Want My Personal Data? Reward Me for It, The New York Times, available at http://www.nytimes.com/2010/07/18/business/18unboxed.html (last visited July 7, 2021).

[11] *See* Il-Horn Hann et al., The Value of Online Information Privacy (Oct. 2002) available at http://www.comp.nus.edu.sg/~ipng/research/privacy.pdf (last visited July 7, 2021); *see also* Tsai, Cranor, Acquisti, and Egelman, The Effect of Online Privacy

45. The information compromised in the Data Breach here is significantly more valuable than the loss of, for example, credit card information because there, victims can cancel or close credit and debit card accounts. The information compromised in this Data Breach—names, dates of birth, driver's license numbers and Social Security numbers, etc.—is difficult, if not impossible, to change.

46. Social Security numbers are among the worst kind of personal information to have stolen because they can be misused so many different ways and are very hard to change. The Social Security Administration stresses that the loss of an individual's Social Security number, as is the case here, can lead to identity theft and extensive financial fraud:

> A dishonest person who has your Social Security number can use it to get other personal information about you. Identity thieves can use your number and your good credit to apply for more credit in your name. Then, they use the credit cards and don't pay the bills, it damages your credit. You may not find out that someone is using your number until you're turned down for credit, or you begin to get calls from unknown creditors demanding payment for items you never bought. Someone illegally using your Social Security number and assuming your identity can cause a lot of problems.[12]

47. And it is no easy task to change or cancel a stolen Social Security number. Plaintiffs and the Class members cannot obtain a new Social Security number

---

Information on Purchasing Behavior, 22 (2) Information Systems Research 254, 254 (June 2011).

[12] Social Security Administration, *Identity Theft and Your Social Security Number*, https://www.ssa.gov/pubs/EN-05-10064.pdf (last visited July 7, 2021).

without significant paperwork and evidence of actual misuse. In other words, preventive action to defend against the possibility of misuse of a Social Security number is not permitted; an individual must show evidence of actual, ongoing fraud activity to obtain a new number.

48. Even then, a new Social Security number may not be effective. According to Julie Ferguson of the Identity Theft Resource Center, "The credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[13]

49. The data stolen in this case commands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "Compared to credit card information, personally identifiable information and Social Security numbers are worth more than 10 times on the black market."[14]

50. By virtue of the Data Breach and unauthorized release and disclosure of the PII/PHI of Plaintiffs and the Class, Defendant has deprived Plaintiffs and the Class

[13] Bryan Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR (Feb. 9, 2015), http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millionsworrying-about-identity-theft (last visited July 7, 2021).

[14] Tim Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, IT World, (Feb. 6, 2015), https://www.networkworld.com/article/2880366/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html (last visited July 7, 2021).

of the substantial value of their PII/PHI, to which they are entitled. Defendant failed to provide reasonable and adequate data security, pursuant to and in compliance with industry standards and applicable law.

51. Defendant violated HIPAA because as a medical billing, coding, and management services provider it is required to secure and protect Plaintiffs and Class members' PII/PHI, because it is "protected health information" as defined under 45 CFR § 160.103. And this information was breached as defined by 45 CFR § 164.402, "the acquisition, access, use, or disclosure of protected health information in a manner not permitted."

52. According to the Federal Trade Commission ("FTC"), unauthorized PII/PHI disclosures wreak havoc on consumers' finances, credit history and reputation, and can take time, money and patience to resolve the fallout.[15]

53. Identity theft associated with data breaches is particularly pernicious due to the fact that the information is made available, and has usefulness to identity thieves, for an extended period of time after it is stolen.

54. As a result, victims suffer immediate and long-lasting exposure and are susceptible to further injury over the passage of time.

[15] *See* Taking Charge, What to Do If Your Identity is Stolen, FTC, at 3 (2012), available at http://www.consumer.ftc.gov/articles/pdf-0009-taking-charge.pdf (last visited July 7, 2021).

55. As a direct and proximate result of Defendant's wrongful actions, inaction and/or omissions, the resulting Data Breach, and the unauthorized release and disclosure of Plaintiffs' and other Class members' PII/PHI, Plaintiffs and the other Class members have suffered, and will continue to suffer, ascertainable losses, economic damages, and other actual injury and harm, including, *inter alia*, (i) the untimely and inadequate notification of the Data Breach, (ii) the resulting increased risk of future ascertainable losses, economic damages and other actual injury and harm, and (iii) the opportunity cost and value of lost time they must spend to monitor their health and financial accounts—for which they are entitled to compensation.

56. As a result of Defendants' failures to prevent the Data Disclosure, Plaintiffs and Class members have suffered, will suffer, and are at increased risk of suffering:

a. The compromise, publication, theft, and/or unauthorized use of their PII/PHI,

b. Out-of-pocket costs associated with the prevention, detection, recovery, and remediation from identity theft or fraud,

c. Lost opportunity costs and lost wages associated with efforts expended and the loss of productivity from addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not

limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft and fraud,

d. The continued risk to their PII/PHI, which remains in the possession of Defendant and is subject to further breaches so long as Defendant fails to undertake appropriate measures to protect the PII/PHI in its possession; and

e. Current and future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, remediate, and repair the impact of the Data Breach for the remainder of the lives of Plaintiffs and Class members.

57. In addition to a remedy for the economic harm, Plaintiffs and the Class Members maintain an undeniable interest in ensuring that their PII/PHI is secure, remains secure, and is not subject to further misappropriation and theft. Plaintiffs therefore requests the injunctive remedies outlined in the Prayer of this Complaint.

58. Plaintiffs bring this lawsuit as a class action on behalf of themselves and all others similarly situated as members of the proposed Class pursuant to Federal Rules of Civil Procedure 23(a), 23(b)(2), 23(b)(3), and 23(c)(4).

59. Plaintiffs seek to represent a proposed Nationwide class defined as follows:

> All persons residing in the United States whose PII/PHI was compromised in the Data Breach that Practicefirst announced on July 1, 2021 and thereafter.

60. Excluded from the Class are: (i) Defendant and its officers, directors, affiliates, parents, and subsidiaries (ii) the Judge presiding over this action and the court staff in this case and any members of their immediate families, and (iii) any other person or entity found by a court of competent jurisdiction to be guilty of initiating, causing, aiding or abetting the criminal activity occurrence of the Data Breaches or who pleads nolo contendere to any such charge.

61. Plaintiffs reserve the right to modify or amend the definition of the proposed Class as additional information becomes available to Plaintiffs.

62. Certification of Plaintiffs' claims for class-wide treatment is appropriate because Plaintiffs can prove the elements of her claims on class-wide bases using the same evidence as would be used to prove those elements in individual actions asserting the same claims.

63. **Numerosity**: The members of the Class are so numerous that joinder of all members of the Class is impracticable. Plaintiffs are informed and believe that the proposed Class include 1,210,688 patients and employees who have been damaged by Defendant's conduct as alleged herein.

64. **Commonality**: This action involves common questions of law and fact, which predominate over any questions affecting individual Class members.

These common legal and factual questions include, but are not limited to, the following:

a. whether Defendant engaged in the wrongful conduct alleged herein;

b. whether the alleged conduct constitutes violations of the laws asserted;

c. whether Defendant owed Plaintiffs and the other Class members a duty to adequately protect their PII/PHI;

d. whether Defendant breached its duty to protect the PII/PHI of Plaintiffs and the other Class members;

e. whether Defendant knew or should have known about the inadequacies of its data protection, storage, and physical property security;

f. whether Defendant failed to use reasonable care and commercially reasonable methods to safeguard and protect Plaintiffs' and the other Class members' PII/PHI from unauthorized theft, release, or disclosure;

g. whether the proper data security measures, policies, procedures, and protocols were in place and operational within Defendant's offices and computer systems to safeguard and protect Plaintiffs' and the other Class members' PII/PHI from unauthorized theft, release or disclosure;

h. whether Defendant breached its promise to keep Plaintiffs' and the Class members' PII/PHI safe and to follow federal data security protocols;

i. whether Defendant's conduct was the proximate cause of Plaintiffs' and

the other Class members' injuries;

j. whether Defendant took reasonable measures to determine the extent of the Data Breach after it was discovered;

k. whether Plaintiffs and the other Class members suffered ascertainable and cognizable injuries as a result of Defendant's conduct;

l. whether Plaintiffs and the other Class members are entitled to recover actual damages; and

m. whether Plaintiffs and the other Class members are entitled to other appropriate remedies, including injunctive relief.

65. Defendant engaged in a common course of conduct giving rise to the claims asserted by Plaintiffs on behalf of themselves and the other Class members. Individual questions, if any, pale by comparison, in both quality and quantity, to the numerous common questions that dominate this action.

66. **Typicality**: Plaintiffs' claims are typical of the claims of the members of the Class. All Class members were subject to the Data Breach and had their PII/PHI accessed by and/or disclosed to unauthorized third parties. Defendant's misconduct impacted all Class members in the same manner and arose from the same set of operative facts and are based on the same set of legal theories.

67. **Adequacy of Representation**: Plaintiffs will fairly and adequately protect the interests of the members of the Class, has retained counsel experienced in

complex consumer class action litigation, and intends to prosecute this action vigorously. Plaintiffs have no adverse or antagonistic interests to those of the Class.

68. **Superiority**: A class action is superior to all other available means for the fair and efficient adjudication of this controversy. The damages or other financial detriment suffered by individual Class members are relatively small compared to the burden and expense that would be entailed by individual litigation of their claims against Defendant. It would thus be virtually impossible for the Class members, on an individual basis, to obtain effective redress for the wrongs done to them. Individualized litigation would create the danger of inconsistent or contradictory judgments arising from the same set of facts and would also increase the delay and expense to all parties and the courts. By contrast, the class action device provides the benefits of adjudication of these issues in a single proceeding, ensures economies of scale and comprehensive supervision by a single court, and presents no unusual management difficulties under the circumstances here.

FIRST CAUSE OF ACTION

Negligence

(On Behalf of Plaintiffs and the Class)

69. Plaintiffs re-allege the paragraphs above as if fully set forth herein.

70. Defendant provides medical management services to medical professionals and as such Defendant is entrusted with its clients' PII/PHI, including

their name, address, email address, date of birth, driver's license number, Social Security number, diagnosis, laboratory and treatment information, patient identification number, medication information, health insurance identification and claims information, tax identification number, employee username and password, employee username with security questions and answers, and bank account and/or credit card/debit card information.

71. Upon receiving the PII/PHI of Plaintiffs and members of the Class, Defendant owed to Plaintiffs and the Class a duty of reasonable care in handling and using this information and securing and protecting the information from being stolen, accessed, and misused by unauthorized parties. Pursuant to this duty, Defendant was required to design, maintain, and test their security systems to ensure that these systems were reasonably secure and capable of protecting the PII/PHI of Plaintiffs and the Class. Defendant further owed to Plaintiffs and the Class a duty to implement systems and procedures that would detect a breach of their security systems in a timely manner and to timely act upon security alerts from such systems.

72. Defendant owed this duty to Plaintiffs and the other Class members because Plaintiffs and the other Class members compose a well-defined, foreseeable and probable class of individuals whom Defendant should have been aware could be injured by Defendant's inadequate security protocols. Defendant actively solicited clients who entrusted Defendant with their PHI/PHI when obtaining and using their

facilities and services for care. To facilitate these services, Defendant used, handled, gathered, and stored the PII/PHI of Plaintiffs and the other Class members. Attendant to Defendant's solicitation, use and storage, Defendant knew or should have known of its inadequate and unreasonable security practices with regard to its computer/server systems and also knew that hackers and thieves routinely attempt to access, steal and misuse the PII/PHI that Defendant received from its clients. As such, Defendant knew a breach of its systems would cause damage to Plaintiffs and the Class members. Thus, Defendant had a duty to act reasonably in protecting the PII/PHI of its clients.

73. Defendant also owed a duty to timely and accurately disclose to Plaintiffs and the other Class members the scope, nature, and occurrence of the Data Breach. This disclosure is necessary so Plaintiffs and the other Class members can take appropriate measures to avoid unauthorized use of their PII/PHI, accounts, cancel and/or change usernames and passwords on compromised accounts, monitor their accounts to prevent fraudulent activity, contact their financial and/or health institutions and insurance providers about compromise or possible compromise, obtain credit monitoring services, and/or take other steps in an effort to mitigate the harm caused by the Data Breach.

74. Defendant breached its duty to Plaintiffs and the Class members by failing to implement and maintain security controls that were capable of adequately protecting the PHI entrusted to it.

75. Defendant also breached its duty to timely and accurately disclose to Plaintiffs and the Class members, that their PII/PHI had been or was reasonably believed to have been improperly accessed or stolen. Plaintiffs and the Class members had no way to protect their information in possession of Defendant.

76. Defendant violated Section 5 of the FTC Act because it engaged in unfair practices by failing to safeguard the PII/PHI of Plaintiffs' and Class members.

77. Section 5 of the FTC Act prohibits unfair practices that affect commerce, including those business practices Defendant engaged in and its failure to protect Plaintiffs and Class members' PII/PHI. Given Defendant's acute awareness of the sensitivity and privacy concerns surrounding the PII/PHI of Plaintiffs and Class members, Defendant was on notice of the likely consequences from such a breach and the impact it would have on Plaintiffs and Class members.

78. Defendant also violated HIPAA privacy laws by failing to protect the sensitive and confidential information of Plaintiffs and members of the Class, provided to Defendant in the course and scope of its business practices as a provider of medical billing, coding, and managed services for healthcare providers. Plaintiffs and members of the Class are the exact demographic HIPAA was enacted to protect. As such, the harm incurred as a result of the Data Breach is the type of harm HIPAA was intended to prevent.

79. Defendant's negligence in failing to exercise reasonable care in

protecting the PII/PHI of Plaintiffs and the other Class members is further evinced by Defendant's failure to comply with legal obligations and industry standards, and the delay between the date of the Data Breach and the time when the Data Breach was disclosed.

80. The injuries to Plaintiffs and the other Class members were reasonably foreseeable to Defendant because laws and statutes, and industry standards require Defendant to safeguard and protect its computer systems and employ procedures and controls to ensure that unauthorized third parties did not gain access to Plaintiffs' and the Class members' PII/PHI.

81. The injuries to Plaintiffs and the other Class members also were reasonably foreseeable because Defendant knew or should have known that systems used for safeguarding PII/PHI were inadequately secured and exposed Plaintiffs' and Class members' PII/PHI to being breached, accessed, and stolen by hackers and unauthorized third parties. As such, Defendant's own misconduct created a foreseeable risk of harm to Plaintiffs and the other Class members.

82. Defendant's failure to take reasonable steps to protect the PII/PHI of Plaintiffs and the members of the Class was a proximate cause of their injuries because it directly allowed thieves easy access to Plaintiffs' and the Class members' PII/PHI. This ease of access allowed thieves to steal PII/PHI of Plaintiffs and the other members of the Class, which could lead to dissemination in black markets.

83. As a direct and proximate result of Defendant's conduct, Plaintiffs and the Class members have suffered theft of their PII/PHI. Defendant allowed thieves access to Class members' PII/PHI, thereby decreasing the security of Class members' financial and health accounts, making Class members' identities less secure and reliable, and subjecting Class members to the imminent threat of identity theft. Not only will Plaintiffs and the members of the Class have to incur time and money to re-secure their bank accounts/health insurance accounts, medical records, and identities, but they will also have to protect against identity theft for years to come.

84. Additionally, Plaintiffs and Class members have suffered and/or will suffer injury and damages, including but not limited to: (i) the loss of the benefit of their bargain with Defendant; (ii) the publication and/or theft of their PII/PHI; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII/PHI; (iv) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest and recover from tax fraud and identity theft; (v) costs associated with placing freezes on credit reports; (vi) anxiety, emotional distress, loss of privacy, and other economic and non-economic losses; (vii) the continued risk to their PII/PHI, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as

Defendant fails to undertake appropriate and adequate measures to protect the PII/PHI of Plaintiffs and Class members in its continued possession; and, (viii) future costs in terms of time, effort and money that will be expended to prevent, detect, contest, and repair the inevitable and continuing consequences of compromised PII/PHI for the rest of their lives.

85. Defendant's conduct warrants moral blame because Defendant actively offered services to Plaintiffs and the Class, wherein it used, handled, processed, and stored the PII/PHI of Plaintiffs and the Class members without disclosing that its security was inadequate and unable to protect their PII/PHI. Holding Defendant accountable for its negligence will further the policies embodied in such law by incentivizing larger healthcare industry professionals and medical service providers to properly secure sensitive patient information and protect the patients who rely on these companies and place their lives in their hands every day.

SECOND CAUSE OF ACTION

Breach of Contracts to which Plaintiffs are third party beneficiaries

(On Behalf of the Plaintiffs and the Class)

86. Plaintiffs re-allege the paragraphs above as if fully set forth herein.

87. Defendant had express or implied contracts or agreements with several medical providers and other medical entities to provide services including secure patient data and records management, retention, retrieval, and storage.

88. Plaintiffs and the members of the Class are intended third-party beneficiaries of contracts entered into between Defendant and these medical entities because it is their PII/PHI that is one of the subjects of the contracts and for which Defendant agreed to provide secure patient data and records management, retention, retrieval, and storage.

89. As alleged previously, Defendant breached these contracts by failing to provide secure or adequate data storage services, resulting in the Data Breach and the theft and misuse of the PII/PHI of Plaintiffs and the Class by unauthorized third persons.

90. Plaintiffs and the members of the Class have a right to recovery for breach because one or more of the parties to these contracts intended to give Plaintiffs and the Class members the benefit of the performance promised in the contracts.

91. As a direct and proximate result of Defendant's breaches of these contracts, Plaintiffs and the Class members suffered the injuries as described in detail above.

THIRD CAUSE OF ACTION

Declaratory and Injunctive Relief

(On Behalf of the Plaintiffs and the Class)

92. Plaintiffs reallege the paragraphs above as though fully set forth herein.

93. As previously alleged, Defendant owes duties of care to Plaintiffs and

Class members that require Defendant to adequately secure the PII entrusted to it.

94. Defendant still possesses the PII pertaining to Plaintiffs and the Class members

95. Defendant has not fully remedied the vulnerabilities in its practices and policies about ensuring the data security of Plaintiffs and the Class members' PII.

96. Accordingly, Defendant has not satisfied its legal obligations and duties to Plaintiffs and the Class members. On the contrary, now that Defendant's lax approach towards data security has become public, the PII/PHI in its possession is more vulnerable than it was prior to announcement of the Data Breach.

97. Actual harm has arisen in the wake of the Data Breach regarding Defendant's obligations and duties of care to provide data security measures to Plaintiffs and the Class members.

98. Plaintiffs, therefore, seek a declaration that Defendant's existing data security measures do not comply with its obligations and duties of care, and to comply with its obligations and duties of care, Defendant must implement and maintain reasonable security measures, including those set forth in the prayer below.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, individually, and on behalf of all others similarly situated, respectfully requests that the Court enter an order:

a. Certifying the Class as requested herein;

b. Appointing Plaintiffs as Class Representative and undersigned counsel as Class Counsel;

c. Finding that Defendant engaged in the unlawful conduct as alleged herein;

d. Enjoining Defendant's conduct and requiring Defendant to implement proper data security practices, specifically:

i. prohibiting Defendant from engaging in the wrongful acts described herein;

ii. requiring Defendant to protect, including through encryption, all data collected through the course of its business in accordance with all applicable regulations, industry standards, and laws;

iii. requiring Defendant to delete, destroy, and purge the PII/PHI of Plaintiffs and the Class members unless Defendant can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiffs and the Class members;

iv. requiring Defendant to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of the personal identifying information of Plaintiffs' and the Class members' PII/PHI;

v. requiring Defendant to engage independent third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors;

vi. requiring Defendant to engage independent third-party security auditors and internal personnel to run automated security monitoring;

vii. requiring Defendant to audit, test, and train its security personnel regarding any new or modified procedures;

viii. requiring Defendant to segment data by, among other things, creating firewalls and access controls so that if one area of Defendant's network is compromised, hackers cannot gain access to other portions of Defendant's systems;

ix. requiring Defendant to conduct regular database scanning and securing checks;

x. requiring Defendant to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the employees' respective responsibilities with handling PII/PHI, as well as protecting the PII/PHI of Plaintiffs and the Class members;

xi. requiring Defendant to routinely and continually conduct internal training and education, and on an annual basis to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;

xii. requiring Defendant to implement a system of tests to assess its respective employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees' compliance with Defendant's policies, programs, and systems for protecting PII/PHI;

xiii. requiring Defendant to implement, maintain, regularly review, and revise as necessary a threat management program designed to appropriately monitor Defendant's information networks for threats, both internal and external, and assess whether monitoring tools are appropriately configured, tested, and updated;

xiv. requiring Defendant to meaningfully educate all Class members about the threats that they face as a result of the loss of their confidential PII/PHI to third parties, as well as the steps affected individuals must take to protect themselves;

xv. requiring Defendant to implement logging and monitoring programs sufficient to track traffic to and from Defendant's servers;

xvi. requiring Defendant to design, maintain, and test its computer systems to ensure that PII/PHI in its possession is adequately secured and protected;

xvii. requiring Defendant to disclose any future data breaches in a timely and accurate manner;

xviii. requiring Defendant to implement multi-factor authentication requirements;

xix. requiring Defendant's employees to change their passwords on a timely and regular basis, consistent with best practices; and

xx. requiring Defendant to provide lifetime credit monitoring and identity theft repair services to Class members.

e. Awarding Plaintiffs and Class members damages;

f. Awarding Plaintiffs and Class members pre-judgment and post-judgment interest on all amounts awarded;

g. Awarding Plaintiffs and the Class members reasonable attorneys' fees, costs, and expenses; and

h. Granting such other relief as the Court deems just and proper.

JURY TRIAL DEMANDED

Plaintiffs, on behalf of themselves and the Class, demand a trial by jury on all issues so triable.

Dated: July 9, 2021

Respectfully Submitted,

By: _____

Gary S. Graifman
KANTROWITZ, GOLDHAMER & GRAIFMAN, P.C.
747 Chestnut Ridge Road
Chestnut Ridge, New York 10977
Telephone: (845) 356-2570
Facsimile: (845) 356-4335
ggraifman@kgglaw.com

Gayle M. Blatt, *Pro Hac Vice* forthcoming
CASEY GERRY SCHENK FRANCAVILLA BLATT & PENFIELD, LLP
110 Laurel Street
San Diego, CA 92101
Telephone: (619) 238-1811
Facsimile: (619) 544-9232
gmb@cglaw.com

Attorneys for Plaintiffs and Putative Class